doi:10.11959/j.issn.1000-436x.2015159

可信度动态感知的间断连接无线网络数据转发机制

吴大鹏，张洪沛，王汝言，刘乔寿
（重庆邮电大学 光通信与网络重点实验室，重庆 400065）

摘 要：提出了一种节点可信度动态感知的间断连接无线网络数据转发机制，节点根据运动过程中所获知的局部网络状态信息以分布式的方式估计其他节点恶意度及协作度，并根据历史信息预测节点的连通状态，进而获知各个节点的信任程度，以合理地选择中继节点，实现高效的数据转发。仿真结果表明，所提出的机制能够有效提高数据传输的可靠性，并大幅降低网络负载率，提高网络资源利用率。

关键词：间断连接无线网络；信任管理；非协作行为；数据转发
中图分类号：TP393 **文献标识码**：A

Dynamical credibility aware data forwarding mechanism for intermittently connected wireless networks

WU Da-peng, ZHANG Hong-pei, WANG Ru-yan, LIU Qiao-shou
(Key Laboratory of Optical Communication and Networks, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: A novel dynamic credibility aware packet forwarding mechanism for intermittently connected wireless networks is proposed. According to the network state information obtained locally by a moving node, the malicious degrees and collaboration degrees of nodes can be obtained in a distributed manner. Meanwhile, based on the node connectivity, the credibility of a node is estimated, furthermore, the relay node can be selected reasonably. Results show that the proposed mechanism can effectively enhance the reliability of data transmission while reducing the network load rate significantly. Thus, the utilization of network resources is improved.

Key words: intermittently connected wireless networks; trust management; non-cooperative behavior; data forwarding

1 引言

间断连接无线网络体系架构下，节点充分利用运动过程所带来的相遇机会，采取“存储-携带-转发”的模式进行通信，有效地克服了端到端路径失效所造成的通信中断问题[1,2]。可见，数据转发过程需要多个节点以协作的方式完成。然而，受社会属性、资源等因素的影响，节点往往会表现出非协作的行为。一般来说，节点的非协作行为可分为自私行为与恶意攻击行为，自私行为表现为节点仅尽力转发与自身关系较强节点相关的数据，而消极对待其他节点的数据，甚至直接丢弃；恶意攻击行为表现在节点不仅会随意丢弃数据，而且会对节点历史信息甚至数据内容进行篡改。目前，间断连接无线网络中常见的恶意攻击行为有 2 种。1）诽谤攻击（BMA, bad mouthing attack）：恶意节点发送关于其他节点的负面推荐信息，以降低其他节点的信任程度；2）奉承攻击（FlA, flattery attack）：恶意节点通过夸大其数据转发数量及历史相遇信息等欺骗其他节点来获得较高信任值。现有研究表明节点

收稿日期：2014-07-26；**修回日期**：2015-03-02
基金项目：国家自然科学基金资助项目（61371097）；重庆市自然科学重点基金资助项目（CSTC2013JJB40001, CSTC2013JJB40006）；重庆邮电大学青年自然科学基金资助项目（A2012-93）；重庆市青年科技人才培养计划基金资助项目（CSTC2014KJRC-QNRC40001）
Foundation Items: The National Natural Science Foundation of China (61371097); Chongqing Natural Science Foundation (CSTC2013JJB40001, CSTC2013JJB40006); The Foundation of Chongqing University of Posts and Telecommunication (A2012-93); Youth Talents Training Project of Chongqing Science & Technology Commission (CSTC2014KJRC-QNRC40001)

万方数据

的恶意攻击行为对网络性能的影响尤为突出[3~5]。然而，受网络拓扑动态变化、节点连接频繁间断等因素的影响，缺少基础设施的间断连接无线网络可信数据传输机制的设计仍面临着很多的困难[6~8]。

针对节点非协作行为对数据转发过程的影响，国内外研究人员提出了不同的解决方案。为了抵御节点的恶意反馈行为，文献[9]建立了线性马尔科夫模型，通过信任程度和信任方差 2 个参数来评估节点之间的信任状态，并利用科尔曼融合方法聚合节点的反馈信息，以此减缓恶意反馈对模型的影响。但所提出的方法假设全部节点均为协作节点，使其扩展性受到较大限制。文献[10]中，节点通过带有时间戳和私钥签名的相遇标签来验证历史相遇信息，然后根据证据理论，对相遇节点的服务能力和信任状态进行估计，从而决定最终的转发者。但在间断连接无线网络中，仅凭相遇信息无法准确地表征节点间的信任状态，且与其他文献类似，其假设网络中的节点为积极协作模式并不合理。文献[11]根据节点积极协作转发信息（PFM, positive forwarding message）验证其转发行为，各个节点采用逐跳的方式将相应的 PFM 反馈到上游节点，通过在 PFM 中的节点签名达到防止恶意节点伪造 PFM 或更改 PFM 的目的。但该机制需要各个节点频繁地交换控制信息，资源开销较大。文献[12]将节点的信任值进行模糊量化，并利用预先设定的门限值通过迭代算法完成恶意节点检测，最终完成节点可信度的评估，进而为数据选择合适的中继节点。但模糊量化的节点信任评级难以准确反映节点信任状态，且预先设定的固定门限值无法满足网络动态性的需求。

显然，上述数据转发机制没有全面考虑节点状态及转发能力，难以合理地为数据选择中继节点。针对上述问题，本文提出一种节点可信度动态感知的间断连接无线网络数据转发机制（DCADF, dynamical credibility aware data forwarding）。根据节点历史行为，综合考虑其社会属性[13,14]，通过恶意度、协作度与连通度 3 个属性估计节点可信任状态，并结合自身感知数据及邻居推荐信息聚合得到节点信任值，进而分布式进行数据转发的决策，从而在有效降低网络负载率基础上，保证数据传输的可靠性，提高网络资源利用率。

2 动态信任管理机制

间断连接无线网络具有分布式特性，信任关系感知过程中需要充分利用节点获知的历史状态信息，此外，间断连接无线网络中的节点分布较为稀疏，单纯依靠节点之间的直接交互信息无法满足信任关系的动态特性，因此，还需要充分考虑来自于其他节点的间接推荐信息，进而，全面且准确地评估节点之间的信任关系。

显然，节点信任状态所涉及的因素较多，难以通过单一的参数全面、准确地反映节点信任状态。因此，本文采用恶意度、协作度和连通度来综合衡量节点的信任状态。其中，恶意度主要表示恶意节点影响数据正常传输的程度，其通过伪造自身或其他节点的信息等手段，非法截获并丢弃网络中正在传输的数据，可见，恶意度能够用来评估节点发动恶意攻击行为的概率，即对节点是否发动恶意攻击行为的信任程度；协作度主要描述了节点自私行为特性，网络中的非协作节点仅为与自身关系紧密的节点提供数据转发服务，对于其他节点数据则根据自身意愿进行转发，可见，节点的自私程度直接决定了其参与数据转发过程的意愿；连通度主要用来衡量节点之间的连接状态，根据社会网络理论可知，节点之间的信任程度与相遇状态直接相关，相遇状态较差节点在给定时间内难以有效地转发数据，因此其可信程度较低，反之相遇状态较好节点间完成有效数据转发的可能性较高，即信任程度较高。对于处于间断连接状态的节点来说，连通度能够从客观上反映节点之间的信任程度。可见，采用上述 3 个参数能够全面地衡量节点信任状态，进而为数据转发做出准确决策。

为了有效地评估节点的信任程度，本文将节点的信任值定义为[0,1]间的变量，其中，0 表示完全不信任，0.5 表示未知，1 表示完全信任。利用 $T_{i,j}(t)$ 表示节点 i 在 t 时刻对于节点 j 信任程度的评估值，如前所述，其估计过程中主要受到恶意度、连通度和协作度 3 个方面因素的影响，具体计算方法如式(1)所示，其中，X 表示信任程度评估过程中所考虑的 3 个信任属性，$T_{i,j}^{x}(t)$ 为节点 i 对 j 关于信任属性 X 的估计值，初始化为 0.5，W^{X} 为对应的权重，且有 $\sum_{X} W^{X}=1$。

$$T_{i,j}(t)=\sum_{X} W^{X} T_{i,j}^{x}(t) \tag{1}$$

2.1 多维信任属性估计

间断连接无线网络具有分布式特性，受限于网

万方数据

络资源，节点无法通过泛洪的方式获知全部网络状态。因此，节点信任值估计的关键问题在于如何利用有限的节点信息近似地估计节点的可信任状态，以有效降低来自网络内部节点的非协作行为造成的影响；同时，节点间的信任关系具有动态性，信任程度估计结果需根据网络状态进行更新，满足实时性需求。

显然，各个节点的历史相遇信息为分布式全局变量，单个节点无法在未获知全局信息的情况下准确感知各节点的运行状况及信任状态。但是，节点可通过自身运动过程所记录的历史信息，辅以与其他节点相遇时获知的历史信息近似估计信任关系。为了准确估计节点状态，网络中每个节点都存储自身与其他节点的历史相遇信息，包括节点 ID 号、相遇时间信息、最小相遇时间间隔和相遇次数，其中相遇时间信息记录了节点间的相遇信息，包括连接建立时间 T_{M_n} 及断开时间 T'_{M_n}。

虽然间断连接无线网络中节点资源有限，然而，随着网络运行不断更新，本文中节点历史相遇信息表始终不会大量占用节点缓存空间并消耗有限的能量资源。其具体分析过程如下：历史相遇信息表中的表项共包括 4 个部分，本文所提出方法中节点 *ID* 表项占 2 byte 空间，其可记录的最大数量为 65 536；根据间断连接无线网络节点相遇状态模型，可知节点在给定较短时间间隔内仅能与一个节点相遇，且节点分布较为稀疏，相遇机会相对较少，同时考虑到后续利用历史相遇时间间隔预测未来连接状态时仅需近 3 次相遇时间间隔信息，因此历史相遇信息表中相遇时间信息表项不断更新，所占用空间的最大值为 3×记录时间值所占空间×节点数量 n_x，其大小低于 $6n_x$ byte；最小相遇时间间隔和相遇次数表项分别为 2 byte；此外，由于节点相遇时仅交换自身的历史相遇信息表，因此交换的数据量不大于 $12n_x$，而节点所保存网络中节点历史相遇信息表的个数不大于 n_x，因此，可知所存储的历史相遇信息表占用 $12n^2{}_x$ byte 空间。当节点传输速率为 a byte/s，额定发射功率为 b mW，接收功率为 c mW，则交换历史相遇信息表项的 2 个节点每次需要额外消耗的能量约为 $(b+c)\frac{12n_x}{a}$ mJ。对于由 100 个采用 Bluetooth2.1+EDR 接口的移动节点组成的网络来说，相遇时交互信息列表的最大数据量为 1.2 KB，两节点需要额外消耗的能量约为 0.96 mJ，历史信息列表占用的最大空间约为 120 KB。间断连接无线网络中节点缓存空间远大于该值，故历史相遇信息表的存储不会造成节点缓存溢出；同时，节点相遇后历史相遇信息表交换过程所耗费的网络存储空间及能量资源较少，对于交互信息转发能耗方面来说，发送一个大小为 200 KB 的数据需要消耗的能量约为 160 mJ，约占总传输能耗的 99%以上，可见，随着所发送数据量的增多，交互信息列表对数据转发性能的影响微乎其微。

如前所述，恶意度主要用来衡量节点发动恶意攻击的概率，即对节点是否发动恶意攻击行为的信任程度，而恶意节点通常会夸大自身或恶意降低正常节点与其他节点相遇次数，以此来截获网络中的合法数据。可见，各个节点所存储的被评估节点 j 与其他节点相遇记录不一致的原因主要包含 2 个方面，分别为节点对相遇状态信息更新不及时和节点 j 恶意篡改了自身的历史相遇信息。因此，可根据节点相遇时交换的历史相遇信息判断节点是否发动了恶意篡改相遇信息的攻击行为，进而估计节点的恶意度。本文利用带有时间戳和私钥签名的相遇标签验证节点的历史相遇信息；同时采用 2 个计数器记录节点的行为，分别为良好行为计数器 $h_{i,j}$ 和不良行为计数器 $g_{i,j}$，当节点 i 与 j 相遇时，首先核对各自历史相遇信息表中节点 j 与其他节点的相遇次数，若一致则 $h_{i,j}$ 加 1，否则，节点 i 比较相遇次数与节点 j 所提供的相遇标签以确定信息不一致的原因，若相遇次数小于相遇标签所记录的数目，则 $h_{i,j}$ 加 1，同时更新自身历史相遇信息表中关于 j 的相遇信息，否则判定节点 j 发动 FLA，不良记录器 $g_{i,j}$ 加 1。为进一步减轻恶意攻击行为对网络性能的影响，检测出 j 的恶意攻击行为后，节点 i 向网络中其他节点发送带有自身签名及时间戳的关于 j 发动攻击的告警信息，各个节点收到并通过验证后标记节点 j 的恶意攻击行为；否则，判断 i 发动诽谤攻击（BMA）。可见，对于动态变化的节点信任关系来说，当节点发动恶意攻击行为时其信任值相应地降低，且下降速度随恶意攻击行为次数的增加而上升，当信任值降低到一定程度后渐趋稳定，具有单调递增特性。因此，本文采用反正切函数描述节点之间信任关系的变化过程，如式(2)所示，在极端恶意和合作的情况下恶意度分别趋于 0 和 1。

万方数据

$$T_{i,j}^{rel,C}(t+\Delta t)=\frac{1}{2}+\frac{1}{\pi}\arctan(h_{i,j}-g_{i,j}) \quad (2)$$

受节点资源有限及理性实体隐私保护等因素制约，节点通常仅为与其社会关系较强的节点转发数据，且转发意愿与社会关系强度直接相关。鉴于节点自私性所导致的数据转发意愿差异，本文采用节点对数据的转发比例估计节点协作度。当且仅当节点 j 与源节点、节点 i 或目的节点为朋友关系时，其协作度 $T_{i,j}^{col,C}(t+\Delta t)=1$。为了能够准确地获知节点在数据转发过程中的状态，本文采用逐跳反馈机制验证中继节点对数据的转发行为。为了避免反馈信息在传输过程中出现丢失，所提出的方法采用下游节点主动反馈的方式，即当其成功接收上游节点的数据之后，立即产生相应的反馈信息并发送至上游节点，继而统计节点对数据的转发状况。当节点 i 转发数据给 j 时，若在给定时间内节点 i 收到节点 j 的反馈信息，表明 j 正确转发了该数据，因此节点 i 关于 j 的正确转发次数 $m_{i,j}$ 加 1；否则错误转发次数 $\mu_{i,j}$ 加 1。进而可得到节点的协作性信任值

$$T_{i,j}^{col,C}(t+\Delta t)=0.5+\frac{1}{2}\left(\frac{m_{i,j}-\mu_{i,j}}{m_{i,j}+\mu_{i,j}}\right)=\frac{m_{i,j}}{m_{i,j}+\mu_{i,j}} \quad (3)$$

显然，选择与目的节点相遇频繁的节点作为中继节点能够显著提高数据传输的有效性，因此节点相遇状态与信任程度直接相关。然而网络中节点的相遇状态由节点的移动模式和活跃度决定，单纯地根据节点间的直接相遇概率无法准确获知相遇状态，因此本文根据历史相遇信息综合考虑节点与目的节点的直接相遇概率和间接相遇概率估计节点连接状态，即通过直接连通度和间接连通度估计节点之间的连通状态。本文将直接连通度表示为 $[0,t+\Delta t]$ 内被评估节点 j 与目的节点 d 的相遇次数与所有节点与 d 最大相遇次数的比值，如式(4)所示，其中，$n_{j,d}$ 表示节点 j 与目的节点 d 的相遇次数，$n_{*,d}$ 表示网络中任意节点与 d 的相遇次数。

$$T_{i,j}^{con,dir}(t+\Delta t)=\frac{n_{j,d}}{\max\{n_{*,d}\}} \quad (4)$$

在间断连接无线网络中，节点相遇时间间隔直接反映了节点连接频繁度。然而由于其具有动态特性，节点下次相遇时间间隔与历史平均相遇时间间隔可能存在较大的偏差，导致平均相遇时间间隔难以准确反映节点连通状态，因此需要根据历史相遇趋势预测节点未来的连接状态以克服上述偏差问题。本文根据历史相遇时间间隔预测下一时刻两者相遇状态，进而准确估计其间接相遇概率，即在节点 j 与 k 相遇后，根据节点 k 与目的节点 d 相遇所经历的时间估计节点 j 与 d 的条件相遇概率。根据节点历史信息得到历史相遇时间间隔后，为了达到准确估计节点相遇状态的目的，本文通过灰色 3 次指数平滑（GM-CES, grey model-cubic exponential smoothing）组合模型对下一刻节点相遇时间间隔进行预测。

在得到下一个时间间隔的预测值 $X(n+1)$ 后，节点 j 与目的节点 d 的条件相遇概率如式(5)所示，其中，$X_{\min}=\min\{X(1),X(2),\cdots,X(n+1)\}$。

$$P_{jkd}(t+\Delta t)=1-\frac{X(n+1)-X_{\min}}{X(n+1)}=\frac{X_{\min}}{X(n+1)} \quad (5)$$

进而，可获知间接连通度

$$\begin{aligned}T_{i,j}^{con,ind}(t+\Delta t)&=P_{j,k}(t+\Delta t)P_{jkd}(t+\Delta t)\\&=P_{j,k}(t+\Delta t)\frac{X_{\min}}{X(n+1)}\end{aligned} \quad (6)$$

显然，对于多副本并行转发的间断连接无线网络来说，节点 j 通过直接或间接方式均可将数据投递到目的节点，即完成数据的转发过程，因此本文考虑将节点的连通度表示为直接连通度与间接连通度中的较大者，即

$$T_{i,j}^{con,C}(t+\Delta t)=\max\{T_{i,j}^{con,dir}(t+\Delta t),T_{i,j}^{con,ind}(t+\Delta t)\} \quad (7)$$

综上所述，在多维信任属性参数的估计过程中，本文利用节点有限的历史信息从不同角度全面地衡量节点可信任状态，并采用告警机制扩散节点的恶意攻击行为，有效地减轻了非协作行为对网络造成的影响。同时在上述可信任状态估计的过程中，所提出机制能够根据节点历史相遇信息预测下一时刻相遇状态，进而估计节点的间接投递概率，从而更加准确地感知节点信任状态。

2.2 信任程度估计

间断连接无线网络中，给定节点与被评估节点之间相遇频率较低，仅凭自身有限的历史信息难以准确感知被评估节点的信任状态。利用邻居节点推荐信息能够有效减缓因节点自身计算误差带来的影响，因此，本文在节点信任状态估计过程中综合考虑了自身直接交互和邻居节点推荐的信任信息，进而有效地减缓由计算误差和节点非协作行为造成的信任值失真。

万方数据

当节点 i 与 j 在 t 时刻相遇之后，在 $t+\Delta t$ 时刻 i 对于 j 关于信任属性 X 的更新方式如式(8)所示，其中，$T_{i,j}^{X,dir}(t+\Delta t)$ 表示 $t+\Delta t$ 时刻节点 i 计算出节点 j 关于信任属性 X 直接信任值，$T_{i,j}^{X,ind}(t+\Delta t)$ 为根据邻居节点推荐信息计算出的间接信任值，权重因子 T_i 为节点 i 的信任值。

$$T_{i,j}^{X}(t+\Delta t)=T_i T_{i,j}^{X,dir}(t+\Delta t)+(1-T_i)T_{i,j}^{X,ind}(t+\Delta t) \quad (8)$$

结合间断连接无线网络特征，本文提出了一种混合式的信任更新机制，即网络中节点相遇或收到更新请求时触发信任值的计算与更新，而当节点长时间未相遇时采用时间触发的更新策略，同时为节省网络资源，当节点相遇但未收到信任信息请求时仅存储相关信息而不进行计算。当节点 i 与 j 相遇时，交换各自的历史相遇信息表，节点 i 根据相应的信息依次计算出 j 关于属性 X 的信任值。本文利用布尔型变量 $C_{i,j}(t)$ 表示节点 i 与 j 在相遇持续时间 Δt 内能否完成必要数据的交换。当 $C_{i,j}(t)$ 为假时，两节点删除本次已交换的信息，并保持最近一次更新的信任值不变。然而当下一时间单元内仍未与 j 有效相遇时，表明两节点的相遇频率降低，短时间内难以通过 j 进行有效的数据传输，且时间越久的信任程度估计结果的可信性越低，即历史信任值已不能准确反映节点 j 的信任状态，因此考虑采用衰减机制更新 j 的信任值，且衰减后信任值的下限为初始值 0.5。信任值衰减的方法如式(9)所示

$$T_{i,j}^{X,dir}(t+\Delta t)=e^{-\lambda_d \Delta t}T_{i,j}^{X,dir}(t) \quad (9)$$

综上，$T_{i,j}^{X,dir}(t+\Delta t)$ 的计算式如下

$$T_{i,j}^{X,dir}(t+\Delta t)=\begin{cases}T_{i,j}^{X,dir}(t), & C_{i,j}(t)=\text{False}\\ T_{i,j}^{X,C}(t+\Delta t), & C_{i,j}(t)=\text{True}\end{cases} \quad (10)$$

同时，本文充分考虑邻居节点的推荐信任值，最后通过加权平均得到节点 j 的信任值；若此时 i 所在社区内无其他邻居节点时，则仅考虑直接信任值，即此刻间接信任值等于当前时间单元内节点的直接信任值。间接信任值的计算方法如式(11)所示，其中，S_i 表示节点 i 除 j 外邻居节点的集合，$|S_i|$ 为集合 S_i 的基数。

$$T_{i,j}^{X,ind}(t+\Delta t)=\begin{cases}T_{i,j}^{X,dir}(t+\Delta t), & |S_i|=0\\ \dfrac{\sum\limits_{K\in S_i}\left\{T_{i,k}^{X}(t)T_{k,j}^{X}(t)\right\}}{\sum\limits_{K\in S_i}T_{i,k}^{X}(t)}, & |S_i|>0\end{cases} \quad (11)$$

当节点 i 与 $k(k\neq j)$ 相遇时，初始状态下，由于不存在给定节点与被评估节点 j 的直接交互信息，因此不更新直接信任值。同时，通过邻居节点的推荐信息更新 j 的信任值，但当未到下一个时间单元或未收到邻居节点关于 j 信任推荐请求时，i 仅收集并存储关于 j 的推荐信任信息，仅当有更新需求时计算 j 的间接信任值。间接信任值 $T_{i,j}^{X,ind}(t+\Delta t)$ 的计算方法如式(12)所示，其中，F_i 为由节点 i 的邻居节点组成的集合，$|F_i|$ 为集合 F_i 的基数。

$$T_{i,j}^{X,ind}(t+\Delta t)=\frac{\sum\limits_{K\in F_i}\left\{T_{i,k}^{X}(t)T_{k,j}^{X}(t)\right\}}{\sum\limits_{K\in F_i}T_{i,k}^{X}(t)} \quad (12)$$

考虑到间断连接无线网络拓扑变化快、网络环境恶劣等因素，权重因子需要根据当前网络状态动态调整，因此本文采用熵权法动态地确定多维信任属性对节点信任状态的影响程度。如前所述，间断连接无线网络中节点的非协作行为对网络性能产生较大影响，在网络实际运行中，受节点移动及非协作节点恶意攻击的影响，节点各个信任属性值将有较大波动，使该参数熵值较小，在评估节点信任值时该参数所提供信息量较大，其对应的权重较大，从而能够更加准确感知节点信任状态。此外本文以 n 个节点提供的关于 3 个属性的信任值作为原始数据，由于原始数据随网络的运行不断更新，因此，通过熵权法可得到各个影响因素随网络状态动态变化的权值，从而能更准确地计算节点信任值。

3　数据转发机制

利用本文所提出的动态信任管理机制，节点可根据网络状况调整计算策略，准确感知邻居节点的转发能力和节点状态，进而，利用所获知的节点信任值评估相遇节点的信任程度，进而对数据进行转发，直到投递成功。可见，为了达到在复杂环境下的间断连接无线网络中可靠传输数据并控制负载率的目的，数据转发过程中的中继节点选择至关重要。

与给定节点相遇的节点包括普通节点和非协作节点 2 类，而非协作节点又包括自私节点与恶意节点。当节点发送数据时，不同属性的相遇节点将执行不同的策略。1）普通节点在收到发送请求后接收数据，并检查自身对该数据的历史转发信息，若缓存中已存储或者该数据已投递成功则直接丢弃，同时向上游节点发送含有丢弃原因的反馈报

万方数据

告；否则，在与其他节点相遇时，根据与相遇节点交互信息以评估其信任值，然后将数据副本转发给其中信任值高于自身且不低于 0.5 的节点，若不存在合适的中继节点，则继续携带数据等待下一次信任值更新，直到转发给满足条件的节点。2）恶意节点收到发送请求并接收到数据后，首先判断该数据的源节点、目的节点或上游节点是否与自身为朋友关系，若满足约束条件，则按照普通节点的转发策略进行处理，否则直接进行丢弃。3）自私节点在收到发送请求时根据对上游节点的转发意愿值选择接收或拒绝接收，当接收到数据后，首先判断数据源节点、目的节点或上游节点是否与自身为朋友关系，若满足条件则按照普通节点转发策略进行处理；否则根据自己对该数据目的节点的转发意愿选择转发或丢弃数据。

网络初始化阶段，设置网络时间单元及信任衰减因子，同时将各节点信任值设置为 0.5，随网络运行节点不断更新自身历史相遇信息及信任值，当两节点相遇时，交换各自历史相遇信息表并根据式(2)计算其恶意度，同时根据对方转发数据状况利用式(3)计算其协作度，此外根据节点相遇次数及相遇时间间隔分别利用式(5)与式(6)估计其直接及间接相遇概率，进而感知其连通度，如式(7)所示；同时向邻居节点请求被评估节点的推荐信任信息，最终根据各信任属性变化状况通过动态加权得到被评估节点信任值，如式(1)所示。在节点信任评估的过程中，如果检测出某节点的恶意攻击行为，则向网络中广播该节点发动恶意攻击的证据信息，以加速网络中恶意节点的检测与孤立。

由于网络中非协作节点的存在对网络性能造成恶劣的影响，且网络的间断连接及动态特性使得通过有限次数的交互难以对节点属性做出准确的判断。然而，根据运行过程中节点转发行为及连接状态所评估的信任度能够直观地反映节点参与数据转发的积极程度及转发能力，因此可根据所评估的节点信任度完成中继节点的合理选择，进而提高数据转发的有效性和可靠性。当节点有数据需要转发时，首先通过恶意度、协作度和连通度计算各相遇节点信任值，同时聚合邻居节点所推荐的间接信任信息评估其信任状态，进而将数据副本转发给相遇节点中信任值高于自身且不低于 0.5 的节点，以完成数据的高效及可靠转发；如果不存在满足条件的节点，则继续携带数据运动等待下次信任更新直到转发给满足条件的节点。当节点需要接收相遇节点发送的数据时，首先检查自身是否为该数据的目的节点，如果是则直接接收；否则，当该节点为普通节点时，接收该数据并依据上述方法选择合适的下一跳中继节点，当该节点为恶意节点时，接收该数据并做丢弃处理以破坏数据的正常传输，当该节点为自私节点时，根据自身与该数据源节点、目的节点、当前携带节点的关系选择接收或拒绝接收，若接收，则根据自身对其转发意愿进行转发处理。若数据 TTL 到期前数据未成功投递，则源节点重新执行上述过程，直到目的节点成功接收。

4 数值分析

本文采用机会网络环境[16,17]（ONE, opportunistic network environment）仿真平台进行网络性能验证，并与典型的数据转发机制 Prophet[18]及 Trust-Thresholds[19]进行对比，以验证所提出机制的有效性。其中，Prophet 作为间断连接无线网络经典的数据转发机制，有效地结合了洪泛和概率预测的思想，网络中每个节点均存储与其他节点的相遇概率，当节点运动过程中与其他节点相遇时，若所遇节点与数据目的节点相遇概率高于自身，则将缓存中对方没有的数据转发给所遇节点，从而更加有效地转发数据；Trust-Thresholds 机制根据历史交互信息通过多维属性评估节点信任值，并结合门限机制选择推荐节点及中继节点，进而完成数据转发的决策。

本文所提出机制根据节点历史相遇及转发信息通过恶意度、协作度和连通度全方面评估节点信任状态，并综合考虑自身感知及邻居推荐信息利用混合式更新机制，准确感知节点可信任状态，进而选择可信度高且传输能力强的节点作为中继，并逐步将恶意节点在网络中孤立，以减少其对网络性能的影响。同时，间断连接无线网络中节点能耗主要消耗在数据传输和侦听过程中，约占总能耗的 95%以上[20]，且节点将 1 bit 数据传输到 10 m 距离需要消耗的能量大约相当于执行 3 000 条计算指令所消耗的能量[21]，而所提出 DCADF 算法在计算节点信任度过程中算法复杂度为 $O(n^2)$，因此，对于 100 个节点组成的网络来说信任度计算过程中需要消耗的能量可以忽略不计；综上，所提出机制中节点交互过程携带及交互的信息列表始终不会占用过的缓存空间及能量资源，且计算信任值对节点能耗等方面的影响也微乎其微。

万方数据

网络性能指标分别为数据投递率、网络负载率及平均传输时延 3 个方面，其中数据投递率表示为成功投递数据数量与总生成数据数量的比值，网络负载率定义为：（转发的消息数−成功投递的消息数）/成功投递的消息数，其反映的是每成功投递一个消息所需要转发消息的次数，而平均传输时延表示为数据从生成到成功投递所经历时间的平均值。仿真参数设置如表 1 所示。

表 1　　仿真参数设置

参数	数值
仿真时间/s	43 200
仿真区域	4 500 m×3 400 m
节点运动模型	社区模型
时间窗口/s	30
节点组/个	6
节点个数/个	96
节点通信方式	蓝牙
节点速度/(m·s^{-1})	5~10
节点缓存空间/MB	5~10
传输范围/m	10
传输速率/(Mbit·s^{-1})	2
数据大小/KB	150~250
数据产生间隔/s	35~40

4.1　恶意节点比例对转发机制影响分析

本节主要验证恶意节点比例变化对所提出 DCADF 机制的影响情况。

图 1 所示为 3 种数据转发机制在恶意节点比例变化情况下的数据成功投递率，从结果可知，随着恶意节点比例的增加，3 种机制的投递率都有所降低。主要原因为恶意节点越多，数据被恶意丢弃及选择不正确路由的概率越大，导致数据投递率降低。同时，上述 3 种数据转发机制中，DCADF 下降的幅度远小于 Prophet，其中 DCADF 的数据投递率比 Prophet 高 20.3%，比 Trust-Thresholds 高 14.1%，且在恶意节点比例增加到 60%时，DCADF 的数据投递率仍能够保持在 66%以上。恶意节点比例对网络负载率的影响如图 2 所示，随恶意节点比例增加，DCADF 和 Trust-Thresholds 的负载率均呈下降趋势，而 Prophet 则逐渐上升。其中，DCADF 的网络负载率比其他 2 种机制平均低 73.5%，且随恶意节点比例不断增加，DCADF 在网络负载率方面的优势越加明显。图 3 为恶意节点比例对平均传输时延的影响情况，上述 3 种机制的平均传输时延都随着恶意节点比例的增加而不断升高。其中，DCADF 的平均传输时延最高，其他 2 种机制时延稍低，DCADF 网络平均时延比 Prophet 高 5.8%，比 Trust-Thresholds 高 19%，而当恶意节点比例超过 35%时，三者时延基本相当。

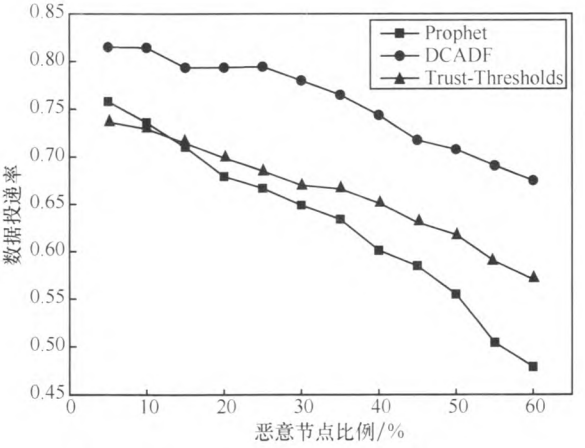

图 1　恶意节点比例变化情况下数据投递率的比较

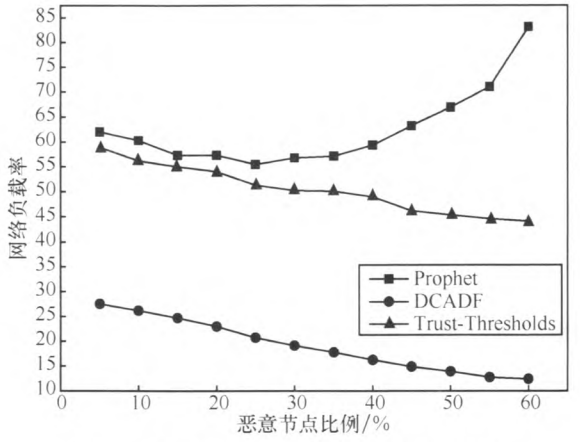

图 2　恶意节点比例变化情况下网络负载率的比较

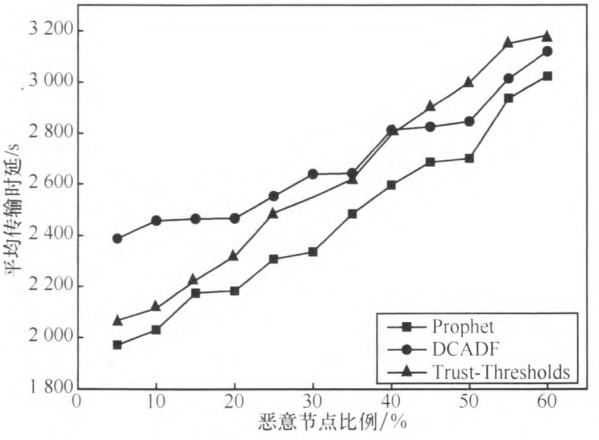

图 3　恶意节点比例变化情况下平均传输时延的比较

万方数据

综上可知，在非协作的网络环境中采用 Prophet 机制进行数据传输时，随着恶意节点的增多，部分可能被成功投递的数据副本被非协作节点截获并被丢弃，使数据投递率下降，同时也浪费了这些数据在转发过程中所消耗的网络资源，携带数据节点不得不复制更多副本以保证数据的有效传输，因此导致网络负载率提高，同时也增大了数据的传输时延。Trust-Thresholds 机制根据节点行为评估其信任状态，同时聚合部分推荐信息得到节点信任值，进而选择信任值大于给定门限节点协助完成数据的转发，该方法能够在一定程度上抵御恶意攻击，然而该机制未考虑节点社会关系，且门限值不能随网络变化进行更新，使其具有一定的局限性。所提出的 DCADF 机制中，节点根据节点历史交互信息全面地评估其他节点信任值，同时当检测到节点篡改历史相遇信息时，判断其发动恶意攻击行为，并向网络中广播节点攻击信息加速恶意节点的检测。此外在信任计算过程中，综合考虑自身感知及邻居推荐信息并利用混合式更新机制，准确感知节点可信任状态，进而选择可信度高且传输能力强的节点作为中继，避免了数据的盲目传输和网络资源的浪费，使在恶意节点较多的情况下仍保持较高的数据投递率和较低的网络负载率。然而由于该机制需要收集并计算其他节点信息，导致其传输时延有一定程度的增加。

4.2 节点缓存对转发机制影响分析

本节主要验证非协作环境下（恶意节点比例30%）节点缓存变化对所提出机制的影响情况。

图 4 所示为 3 种数据转发机制在不同缓存情况下的数据投递率，从图中曲线可知：随着节点缓存的增加，3 种机制的投递率都呈明显的上升趋势。且上述数据转发机制中，DCADF 的平均数据投递率最高，其中比 Prophet 高 17.9%，比 Trust-Thresholds 高 12.6%，且随节点缓存进一步增加，上述 4 种机制的数据投递率渐趋平稳。节点缓存对网络负载率的影响如图 5 所示，随节点缓存大小的增加，上述 3 种数据转发机制的负载率均呈下降趋势并渐趋稳定，且 DCADF 的网络负载率远小于其他 2 种机制。这充分验证了相比其他 2 种机制 DCADF 在节省网络资源方面的优势。图 6 给出了节点缓存对平均传输时延的影响情况，3 种机制的平均传输时延都随着节点缓存的增加而逐渐升高。其中，Prophet 的平均传输时延最高，DCADF 次之，而 Trust-Thresholds 最低。随着节点缓存增加，3 种算法的平均传输时延渐趋稳定。

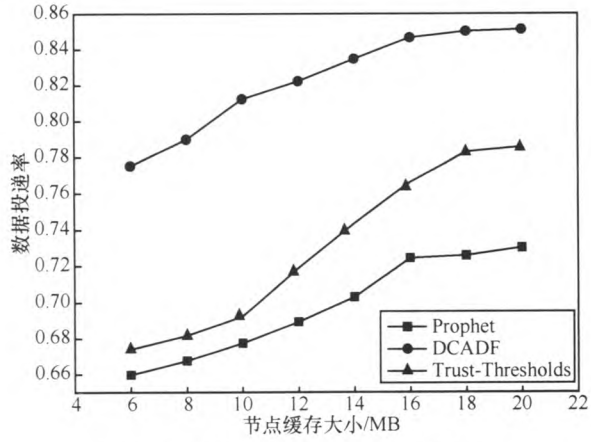

图 4 节点缓存变化情况下数据投递率的比较

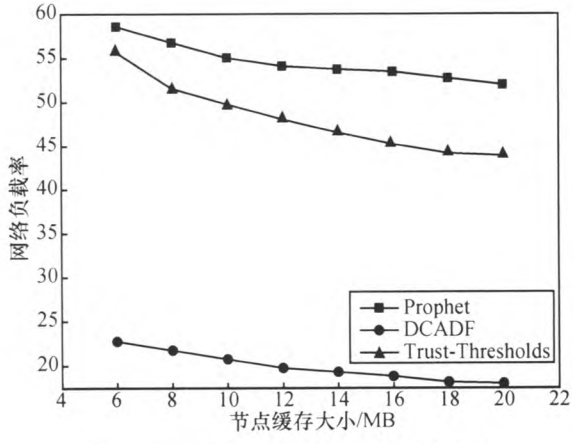

图 5 节点缓存变化情况下网络负载率的比较

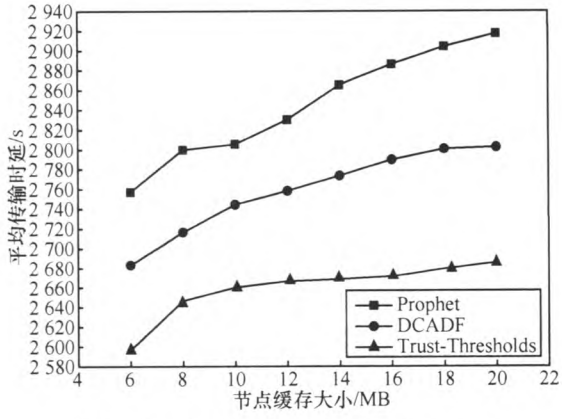

图 6 节点缓存变化情况下平均传输时延的比较

综上可知，在非协作的网络环境中进行数据传输时，随着节点缓存的增大，节点能够存储更多的数据副本，进而提高数据的成功投递率，同时使网络负载率具有一定程度的下降。然而由于部分可能被成功投递的数据副本被恶意节点截获并丢弃，导

万方数据

致数据投递率下降及传输时延的增加。相比 DCADF，其他 2 种机制的投递率均偏低，其中当节点缓存小于 8 MB 时，Prophet 受缓存限制其投递率略低于 Trust-Thresholds。作为一种高效的信任管理机制，Trust-Thresholds 机制能够根据节点行为评估其信任状态，然而由于缺乏有效的检测及告警机制，且不能随网络状况动态改变信任门限值，使其性能未能有更进一步提升。DCADF 由于综合考虑节点恶意度、协作度评估其信任状态，同时结合直接连通度与间接连通度综合选取中继节点，并根据网络状况动态调整评估策略，因此能够保证较高的数据投递率和较低的网络负载率，然而由于信任计算、聚合及传播过程需要耗费较多时间，导致了平均传输时延的增加。

5　结束语

为了实现在非协作的间断连接无线网络中进行可靠的数据传输，本文提出了一种节点可信度动态感知的数据转发机制。首先根据节点交互信息估计其信任值，并利用历史信息预测未来状态，进而聚合邻居推荐信息全面估计节点信任状态，从而合理的选择中继节点完成数据的转发。仿真结果表明，与传统路由机制及信任管理机制相比，所提出的 DCADF 机制能够在非协作环境中保证较高的数据投递率，并大幅降低网络负载率，有效提高了网络可靠性及资源利用率。

间断连接无线网络中，节点的频繁移动以及基础设施的缺乏给信任管理机制的设计带来较大的挑战，尤其是针对节点性质的判定方法。一般来说，复杂度较高的迭代算法能够提高检测的准确度，然而，在资源受限的间断连接无线网络中，此类算法将引发极高的能耗使网络的生存时间降低，导致网络的可用性变低。因此，在后续的研究中将继续研究复杂网络环境中节点性质的检测方法以及相应的能耗问题，以提高间断连接无线网络中数据传输的可靠性和网络的生存性，进而优化网络资源，提高网络可用性。

参考文献：

[1] DARSHANA P, VANDANA V. Security enhancement of AODV protocol for mobile ad hoc network[J]. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2013, 2(1): 317-321.

[2] ZHU Y, XU B, SHI X H, *et al*. A Survey of social-based routing in delay tolerant networks: positive and negative social effects[J]. IEEE Communications Surveys & Tutorials, 2013, 15(1): 387-401.

[3] MANAM V K C, MAHENDRAN V, MURTHY C S R. Performance modeling of DTN routing with heterogeneous and selfish nodes[J]. Wireless Networks, 2014, 20(1): 25-40.

[4] LI Y, SU G, WANG Z. Evaluating the effects of node cooperation on DTN routing[J]. AEU-International Journal of Electronics and Communications, 2012, 66(1): 62-67.

[5] RESTA G, SANTI P. A framework for routing performance analysis in delay tolerant networks with application to noncooperative networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(1): 2-10.

[6] ZHU H, DU S, GAO Z, *et al*. A probabilistic misbehavior detection scheme towards efficient trust establishment in delay-tolerant networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(1): 22-32.

[7] ANUSHA T, RAO N S. Improving the trust and adversary detection process for delay-tolerant networks[J]. International Journal of Computer Science and Mobile Applications, 2013, 1(5): 44-50.

[8] GOVINDAN K, MOHAPATRA P. Trust computations and trust dynamics in mobile adhoc networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2012, 14(2): 279-298.

[9] WANG X, LIU L, SU J. Rlm: a general model for trust representation and aggregation[J]. IEEE Transactions on Services Computing, 2012, 5(1): 131-143.

[10] LI F, WU J, SRINIVASAN A. Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets[A]. IEEE INFOCOM 2009[C]. 2009. 2428-2436.

[11] LI N, DAS S K. A trust-based framework for data forwarding in opportunistic networks[J]. Ad Hoc Networks, 2011, 11(4): 1497-1509.

[12] AYDAY E, FEKRI F. An iterative algorithm for trust management and adversary detection for delay-tolerant networks[J]. IEEE Transactions on Mobile Computing, 2012, 11(9): 1514-1531.

[13] HUI P, CROWCROFT J, YONEKI E. BUBBLE rap: social-based forwarding in delay-tolerant Networks[J]. IEEE Transactions on Mobile Computing, 2011, 10(11): 1576-1589.

[14] EYUPHAN B, BOLESLAW K. Exploiting friendship relations for efficient routing in mobile social networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(12): 2254-2265.

[15] CHEUNG S, SUN Y, ABERER K, *et al*. Guest editorial: special issue on privacy and trust management in cloud and distributed systems[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(6): 835-837.

[16] KERÄNEN A, OTT J, KÄRKKÄINEN T. The one simulator for dtn protocol evaluation[A]. Proceedings of the 2nd International Conference on Simulation Tools and Techniques. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) [C]. 2009. 1-10.

[17] THOMPSON N, NELSON S C, BAKHT M, *et al*. Retiring replicants: congestion control for intermittently-connected networks[A]. IEEE

万方数据

INFOCOM[C]. 2010.1-9.

[18] LINDGREN A, DORIA A, SCHELEN O. Probabilistic routing in intermittently connected networks[J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2003, 7(3): 19-20.

[19] CHEN I, BAO F, CHANG M, *et al*. Dynamic trust management for delay tolerant networks and its application to secure routing[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 25(5): 1200-1210.

[20] ZHOU H, CHEN J, ZHAO H, *et al*. On exploiting contact patterns for data forwarding in duty-cycle opportunistic mobile networks[J]. IEEE Transactions on Vehicular Technology, 2013, 62(9): 4629-4642.

[21] 孙利民, 李建中, 陈渝. 无线传感器网络[M]. 北京: 清华大学出版社, 2005.
SUN L, LI J Z, CHEN Y. Wireless Sensor Networks[M]. Beijing: Tsinghua University Press, 2005.

作者简介：

吴大鹏（1979-），男，黑龙江大庆人，重庆邮电大学教授、硕士生导师，主要研究方向为泛在无线网络、社会计算、互联网服务质量控制。

张洪沛（1988-），男，河南南阳人，重庆邮电大学硕士生，主要研究方向为间断连接无线网络、信任管理机制、服务发现。

王汝言（1969-），男，湖北浠水人，博士，重庆邮电大学教授、博士生导师，主要研究方向为泛在网络、多媒体信息处理等。

刘乔寿（1979-），男，云南曲靖人，重庆邮电大学副教授，主要研究方向为泛在无线网络、物联网等。

万方数据